iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improving Security Rate with Cognitive Radio Networks Using Cooperative Secure Resource Allocation

Saranya.M[1], Vinayagam.T.A[2], Divya.M[3]
Sri Venkateshwara College of Engineering and Technology, India

Abstract— ***A secure communication in cognitive radio networks, where the secondary users are allowed to access the spectrum of the primary users as long as they preserve the secure communication of PU in the presence of malicious eavesdroppers. The secondary users will uses the two hops in which the secondary user will act as a relay set and the friendly jammer for the primary user and the eavesdroppers. In this new setup, the time duration for each hop, the power transmissions of all nodes in CRN, and relay selection at the second hop are allocated in such a way that the secrecy rate of the SU is maximized subject to the minimum required PU's secrecy rate. I use the digital signature algorithm for wireless system and optimize the power allocation, time allocation and relay selection problems. I also provide an intrusion detection system to detect the users who act as a false transmitter or receiver. The power allocation problem can be transformed into generalized geometric programming (GGP) model via scaled algorithm and it can be solved very efficiently.***

Index Terms—Cognitive radio networks, ergodic and instantaneous resource allocation, generalized geometric programming (GPP), secure communication.

I. INTRODUCTION

SPECTRUM sharing through cognitive radio network (CRNs) is a promising approach to increase the spectrum efficiency for next generation of wireless communication networks [1] where the unlicensed/secondary users (SUs) are allowed to access the spectrum of primary users (PUs) subject to maintaining the quality of service (QoS) of PUs. The SUs can simultaneously utilize the licensed spectrum of PUs if the resulting interference on the PUs' receivers is kept under a predefined threshold. Similar to any wireless network, security against overhearing of the third parties, referred to as eavesdroppers, is one of the important issues in CRNs. Recently, physical layer security introduced by [2], is drawing a lot of attentions in which the objective is to maximize the secrecy rate defined as the achievable rate from the transmitter to the legitimate receiver minus the rate overheard by eavesdropper. Obviously, when the channel gain between transmitter and its corresponding receiver is less than the channel gain between transmitter and eavesdropper, the secrecy rate is equal to zero. For non-cognitive networks, achieving a non-zero secrecy rate is studied from different aspects in non-cooperative [3] as well as cooperative frameworks including cooperative relaying [4], cooperative jamming [5], and jointly cooperative jamming and relaying [6]. Cooperative jamming, also known as friendly jamming, creates interference by legitimate network nodes,transmitting noise [7], [8] or codewords [9], [10], so as to impair the eavesdroppers ability to decode the confidential information, and thus, increase secure communication rates between each legitimate transmitter and receiver. This problem in cognitive case has been considered in [8], [11]–[17]. Information theoretic aspect of secrecy rate are addressed in [11], [12] where the effect of trustworthy SUs to increase the secrecy rate of PU is investigated. Resource allocation (RA) problems to maximize the secondary secrecy rate underlay approach in different MIMO transmission modes are investigated in [13]–[15]. A similar study in a cooperative relaying framework has been proposed in [16]. The effect of friendly jammer in the underlay cognitive radio network was studied in [8]. In [17], the secrecy rate of PU is maximized in MIMO channels subject to the minimum required shannon rate of SU. In RA problems associated to [13]- [17], the objective is to provide secure transmission for either primary or secondary users subject to the imposed constraints by PUs and particular, interference threshold constraint in underlay. However, in CRNs, secure communication for both PUs and SUs is of high importance and previously proposed settings do not accommodate secure communications for both primary and secondary users. In this paper, we propose a cooperative paradigm for secure communication in CRNs in which secure communications for both primary and secondary services are simultaneously provided. This goal is achieved by taking advantage of the interference caused by the secondary user activity to reduce the primary service overhearing by the eavesdroppers. From primary service perspective, this transforms the possibly

disturbing secondary service activities into a beneficial network element. The RA problem for the proposed setup is written as an optimization problem with the objective of maximizing the SU's secrecy rate subject to guaranteeing a given PU's secrecy rate. It can be seen that the feasibility set of this problem highly depends on the channel gains, referred to as channel state information (CSI) between network nodes, i.e., the PU the SU and eavesdroppers, as well as the required primary secrecy rate. Consequently, there is a good chance that the RA problem is not feasible meaning that the secondary secrecy rate is zero. To make the problem feasible, we propose to expand the feasibility set by deploying relays within the secondary network. Then, at any primary service transmission period, the transmission of SU is done in two hops. In the first hop, the secondary transmitter (ST) sends the information to the set of relays and the secondary receiver (SR) acts as a friendly jammer to interfere the overhearing of eavesdroppers. In the second hop, one of the relays is selected to transmit the information to the SR and the ST acts as a friendly jammer. This setup can be considered as a joint cooperative jamming and relaying scheme where the RA problem includes power allocation of all nodes (i.e., the ST, the SR and relays), relay selection for the second hop, and time allocation for each hop.

We show that the expansion of the feasibility set results in chance of having a non-zero secondary secrecy rate while maintaining a given primary secrecy rate.

The proposed RA problem is non-convex and we apply the scaled algorithm in [18] to transform it into a convex one with respect to each set of variables. We show that this transformation can be represented as a generalized geometric programing (GGP) problem which can be solved very efficiently using existing approaches such as interior-point algorithms [19]. We consider two cases of RA problems: Instantaneous resource allocation (IRA) and ergodic resource allocation (ERA). In the former case, we assume the availability of perfect CSI between any transmitter and receiver within the network. Consequently, for each new set of CSI values, the IRA problem has to be solved [20]. In the latter case, allocations are made based on the long term channel distribution information (CDI). Apparently, ERA exhibits a less computational complexity compared to that of IRA. However, the drawback of ERA is that we can guarantee a secrecy rate for PUs only in average sense not instantaneously, meaning that there exists the probability that the secrecy rate of PU is below than its predefined threshold called outage probability of primary secrecy rate. To deal with this issue, we introduce a modified ERA problem where the outage probability of primary secrecy rate can be kept below any value of interest.

The last challenge for our setup is the assumption of availability of perfect values of CSI between different nodes of the network is not realistic, mainly due to the existence of malicious eavesdroppers which are not supposed to cooperate with SUs and PUs to provide the CSI values. We approach this challenge by considering imperfect values for CSI and propose the robust counterparts of the RA problems. For the IRA problem, we apply the worst case robust optimization to guarantee the PU's secrecy rate under any condition of error. For The ERA problem, we show that the marginal channel distribution can be used to tackle the uncertainty [21], [22].

An important aspect of the proposed paradigm is that replacing the conventional interference threshold constraint by the primary secrecy rate constraint not only does not decrease the secondary secrecy rate with respect to the conventional case, but can also provide significantly higher secondary secrecy rate. The rest of this paper is organized as follows. In Section II, the system model is discussed in details. In Section III, the RA problem is introduced and the solution of IRA is presented. Section IV includes two cases of ERA followed by Section V, where the imperfect CSI is considered for both IRA and ERA. Section IV provides simulation results and Section IIV concludes the paper.

II. NETWORK SETUP

A. System Model

We consider an interference limited CRN in which there exist a primary network with single transmitter and receiver, a trustworthy secondary network, and a set of eavesdropping malicious nods i.e., $E = \{1, \cdots, E\}$, which attempt to overhear the primary and secondary messages. The primary transmitter (PT) wants to send confidential data to its corresponding receiver in its own available spectrum B. The primary network allows the ST to access its spectrum as long as the secrecy rate between PT and primary receiver (PR) is higher than a predefined threshold donated by $\text{CPT}\rightarrow\text{PR}_{\min}$.

In our system model, we assume decode and forward (DF) relaying strategy where the relay nodes are assumed to operate in half-duplex mode, i.e., they do not transmit and receive simultaneously in the same frequency band. Accordingly, the transmission between the secondary transmitter and receiver occurs in two hops: in the *first hop*, the ST transmits data to the selected relay node; and in the *second hop*, the selected relay node sends data to the SR.

The secondary transmitter enjoys this opportunity to transmit messages securely to the secondary receiver, where the secondary network consists of a ST and its corresponding SR, and a set of intermediate nodes i.e., $R = \{1, \cdots, R\}$.

The intermediate nodes help the ST to transmit the data into the SR as a relay set, as shown in Fig. 1. Accordingly, the transmission between the ST and the SR occurs in two hops:

First hop: Transmission from the ST to relays with duration $T1$ where the SR acts as a friendly jammer for the primary service to interfere with eavesdropper's overhearing.

Second hop: Transmission from one selected relay to the SR with duration $T2$ where $T = T1 + T2$ is the transmission period of the primary service and the ST acts as a friendly jammer for the PT to decrease the eavesdroppers rate.

For both hops, the transmit power of the PT is fixed to PPT. The maximum power of the ST and SR are equal to PST max and PSR max,

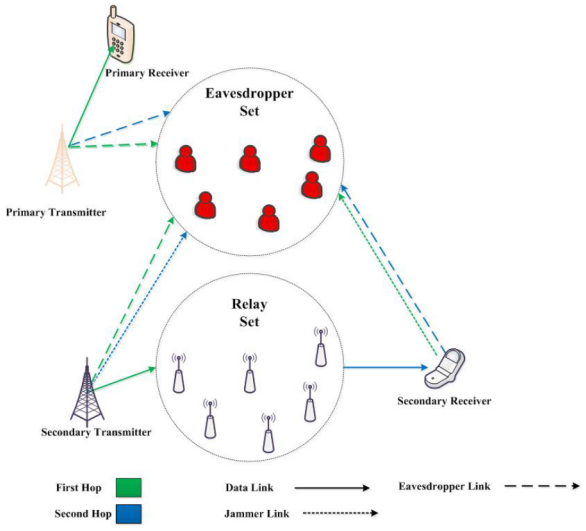


Fig. 1. System model of cooperative CRN with secure transmission.

Throughout this paper, the superscripts 1 and 2 are utilized for any parameters in the first and second hops and $m \rightarrow n$ is used to denote a correspondence between a transmitter named m and a receiver named n. Accordingly, for transmission from transmitter m to receiver n, $\gamma im \rightarrow n$ and $ci\ m \rightarrow n$ denote the corresponding SINR and secrecy rate where superscript $i \in \{1, 2\}$ shows the transmission occurs in hop i. We also assume that $N0B$ is the white gaussian noise power over bandwidth B which is equal for all users in CRN. Also, $hm \rightarrow n$ denotes the CSI between transmitter m and receiver n which is assumed to be fixed during one transmission period. For the case of imperfect CSI, $hm \rightarrow n$, $\bar{}hm \rightarrow n$ and $\hat{}hm \rightarrow n$ show the exact, estimated and error value of the CSI between transmitter m and receiver n. When the CSI is perfect, $hm \rightarrow n = \bar{}hm \rightarrow n$.

The corresponding gain notations are summarized in Table I.

B. *First hop*

At the first hop, the SINR of the PR is computed as

$\mathrm{PT} \rightarrow \mathrm{PR}(\boldsymbol{p}1) = \mathrm{PPT}h\mathrm{PT} \rightarrow \mathrm{PR}\ N0B + I1$

where $\boldsymbol{p}1 = [p1\mathrm{ST}, p1\mathrm{SR}]$ in which

$p1\mathrm{ST}$ is the transmit power of the ST and $p1\mathrm{SR}$ is the transmit power of the SR at the first hop when it acts as a jammer for eavesdroppers; and$I1$ PR is the induced interference in the PR, which is equal to

$I1\mathrm{PR} = I1\mathrm{SR} \rightarrow \mathrm{PR} + I1$

$\mathrm{ST} \rightarrow \mathrm{PR} = p1\mathrm{SR}$

$h\mathrm{SR} \rightarrow \mathrm{PR} + p1\mathrm{ST}$

$h\mathrm{ST} \rightarrow \mathrm{PR}$. Similarly,

SINR for the first hop at eavesdropper e is equal to$\gamma 1$

$\mathrm{PT} \rightarrow \mathrm{e}(\boldsymbol{p}1, e) = \mathrm{PPT}h\mathrm{PT} \rightarrow \mathrm{e}N0B + I1\mathrm{PT} \rightarrow \mathrm{e}$,

Where

$I1\mathrm{PT} \rightarrow \mathrm{e} = I1$

SR→e + $I1$
ST→e = $p1$
SRhSR→e + $p1$
SThST→e. In this hop, the secrecy rate of PU is equal to
$c1$PT→PR($\boldsymbol{p}1$) = min$e$PT→PR($\boldsymbol{p}1$, e)
where
$c1$PT→PR($\boldsymbol{p}1$, e) =$T1$
$T1 + T2 \times \log2(1 + \gamma 1\text{PT}\rightarrow\text{PR}(\boldsymbol{p}1)) - \log2(1 + \gamma 1\text{PT}\rightarrow\text{e}(\boldsymbol{p}1, e)\_+$
.
Simultaneously in the secondary network, the ST sends the data to all relay nodes and the SINR of relay r is
$\gamma 1\text{ST}\rightarrow r(\boldsymbol{p}1, r) = p1\text{ST}h\text{ST}\rightarrow rN0B + I1, \ \forall r \in R$, (4)
where $I1$
$r = I1\text{SR}\rightarrow r + I1$
PT→r = pSRhSR→r +PPThPT→r, and the SINR received at the eavesdropper e is equal to
$\gamma 1\text{ST}\rightarrow e(\boldsymbol{p}1, e) = p1\text{ST}h\text{ST}\rightarrow eN0B + I1\text{ST}\rightarrow e,$
where
$I1$ST→e = $I1$
SR→e + $I1$
PT→e = $p1$
SRhSR→e + PPThPT→e.
Therefore, the secrecy rate of secondary user is
cST→r($\boldsymbol{p}1$, r)=min$e \in E_c\text{ST}\rightarrow r(\boldsymbol{p}1, e)$
where
cST→r($\boldsymbol{p}1$, r, e) $T1$
$T1 + T2 \times \log2(1 + \gamma 1\text{ST}\rightarrow r(\boldsymbol{p}1, r)) - \log2(1 + \gamma 1\text{ST}\rightarrow e(\boldsymbol{p}1, e))$

C. *Second hop*

In this phase, the SINR of the PR is equal to
$\gamma 2\text{PT}\rightarrow\text{PR}(\boldsymbol{p}2, r) = \text{PPT}h\text{PT}\rightarrow\text{PR}N0B + I2\text{PR}(r)$
where
$\boldsymbol{p}2 = [p2\text{ST}, \mathbf{p}2r]$ in which $p2$
ST is the transmit power of the
ST in the second phase and
$\mathbf{p}2r = [p21, \cdots, p2R]$ is the vector
of transmit powers of relay nodes where
$p2r$ is the transmit
power of relay r at the second hop, and
$I2\text{PR}(r) = I2\text{ST}\rightarrow\text{PR} + I2$
$r\rightarrow\text{PR} = p2$
SThST→PR + $p2r$
$hr\rightarrow$PR, for all $r \in R$. The SINR at
eavesdropper e is equal to
$\gamma 2\text{PT}\rightarrow\text{e}(\boldsymbol{p}2, r, e) = \text{PPT}h\text{PT}\rightarrow\text{e}N0B + I2\text{PT}\rightarrow\text{e}(r)$
where
$I2\text{PT}\rightarrow e(r) = I2\text{ST}\rightarrow e + I2$
$r\rightarrow e = p2\text{ST}h\text{ST}\rightarrow e + p2r$
$hr\rightarrow e$, forall $r \in R$. Now, the secrecy rate at the second hop from the
PT to the PR is given by
$c2\text{PT}\rightarrow\text{PR}(\boldsymbol{p}2, r) = \text{min}\_c2$

PT→PR(**p**2, *r*, *e*) (9)
where
*c*2PT→PR(**p**2, *r*,*e*) =*T*2*T*1 +*T*2× log2(1 + *γ*2PT→PR(**p**2, *r*)) − log2(1 + *γ*2PT→e(**p**2, *r*,*e*))

Consequently, the secrecy rate of the PU is obtained as
*c*PT→PR(**p**, *r*) = *c*1
PT→PR(**p**1, *r*) + *c*2
PT→PR(**p**2, *r*), (10)
Where
p = [**p**1, **p**2]. At this hop, in the secondary network, the relays send the message from the ST to the SR and the SINR of the SR from relay *r* is*γ*2*r*→SR(**p**2, *r*) =*prhr*→SR*N*0*B* + *I*2
SR (11)
where *I*2
SR = *I*2
ST→SR + *I*2
PT→SR = *p*2
ST*h*ST→SR + PPT*h*PT→SR.
Also, the eavesdropper SINR from relay *r* is*γ*2*r*→*e*(**p**2, *r*, *e*) =*prhr*→*e*
*N*0*B* + *I*2*r*→*e*, ∀*r* ∈ *R*, (12)
in which *I*2*r*→*e* = *I*2ST→*e* +*I*2
PT→*e* = *p*2ST*h*ST→*e* +PPT*h*PT→*e* forall *r* ∈ *R* and
*c*2*r*→SR(**p**2, *r*) = min*e*∈*E*

_
*c*2*r*→SR(**p**2, *r*, *e*)
where
*c*2*r*→SR(**p**2, *r*, *e*) =*T*2
*T*1 + *T*2×log2(1 + *γ*2*r*→SR(**p**2, *r*)) − log2(1 + *γ*2*r*→*e*(**p**2, *r*, *e*)) (13)

Finally, the secondary secrecy rate will be
*c*ST→*r*→SR(**p**, *r*) =min*c*1ST→*r*(**p**1), *c*2*r*→SR(**p**2) (14)
Similar to other works in literature, in this paper we assume that the CSI values between different nodes of the network are available to the secondary transmitter to be used in allocating the resources. We then consider the case where such CSI values are imperfect and derive corresponding secrecy rates.
We also assume that eavesdroppers use single-user decoding,
i.e., while decoding primary user data, secondary user data is considered as noise and vise versa.

III. INSTANTANEOUS RESOURCE ALLOCATION PROBLEM AND ITS SOLUTION

A. *The RA Problem*

From the setup of Section II, the secondary secrecy rate
depends on the following parameters which are selected from
their corresponding sets:
1) *T*1 and *T*2 chosen from *T* =*T*1, *T*2| *T*1 > 0, *T*2 >0, *T*1 + *T*2 = *T*
which is the set of time intervals for thefirst and second hops;
2) The transmit power of nodes in two hops i.e., **p**1 and **p**2,picked up from the set *P* =**p**| **0** _ **p** _ **p**max
where1
pmax = [PSTmax, PSR
max, **p**Relaymax];
3) The relay *r* which is deployed in the second hop to transmit

the information to the SR for which the corresponding set is
denoted by ϕ where $\phi = \boldsymbol{\rho} | \boldsymbol{\rho}.\mathbf{1}T = 1$
in which $\boldsymbol{\rho} = [\rho 1, \cdots, \rho R]$ and $\rho r = \{0, 1\}$ for all relay nodes, implying that
only one relay is selected for transmission to the SR. Now,
the RA problem of the secondary network.

B. Feasibility Condition

As mentioned before, one concern for secrecy rate is that it might be zero depending on the value of hPT→PR and hPT→e. Now, we want to show how by extending the set of optimization variables, we can increase the chance that(15) is feasible, meaning that the primary secrecy rate is nonzero and greater than CPT→PRmin . In line with existing literature on interference limited networks, the following discussion on feasibility is based on the assumption of high SINR at the PR and the SR [23].
For the case that there is no SU in the network, (15) is feasible, if the following optimization problem has a solution [24]

TABLE II
ALGORITHM I
Step1: Initialize $L\mathbf{max}$, and set $l = 0$,
Step2: Initialize $\boldsymbol{p}0$ and $\boldsymbol{\rho}0$ and T 1 ,
Step3: Repeat:
Step4: Find a power allocation with $\boldsymbol{\rho} = \boldsymbol{\rho}l$ and$T1 = T$ 1, using the algorithm proposed in subsection III.C.1,
Step5: Find a relay selection with $\boldsymbol{P} = \boldsymbol{P}l$ an$T1 = T\,l1$, using the algorithm proposed in subsection III.C.2,
Step6: Find a time allocation with $\boldsymbol{P} = \boldsymbol{P}l$ and $\boldsymbol{\rho} = \boldsymbol{\rho}l$, using the algorithm proposed in subsection III.C.3,
Step7: $l = l + 1$, until $\_\boldsymbol{P}l - \boldsymbol{P}l-1\_ < \varepsilon$ or $l = L$max.

C. The Iterative Algorithm

It can be seen that (15) is a non-convex optimization problem with respect to **Ξ**. To solve the problem, we utilize the iterative algorithm introduced by [25] where the
optimization variables are divided into independent sets of variables. Then, corresponding to each set of variables, the new optimization problem is solved. For example, for ou problem, we have three sets of optimization variables: 1) P,
2) T , 3) ϕ. The optimization problem can be decomposed into three subproblems: 1) Power allocation subproblem, 2) Relay selection subproblem, 3) Time allocation subproblem. The iterative algorithm to solve these subproblems is summarized in Table II. In this algorithm, l is the current iteration number and the superscript l indicates that the associated variable is obtained after the lth iteration. In [25], it has been shown that the iterative algorithms converges to a near optimal solution of (15) if each subproblem can be solved optimally.

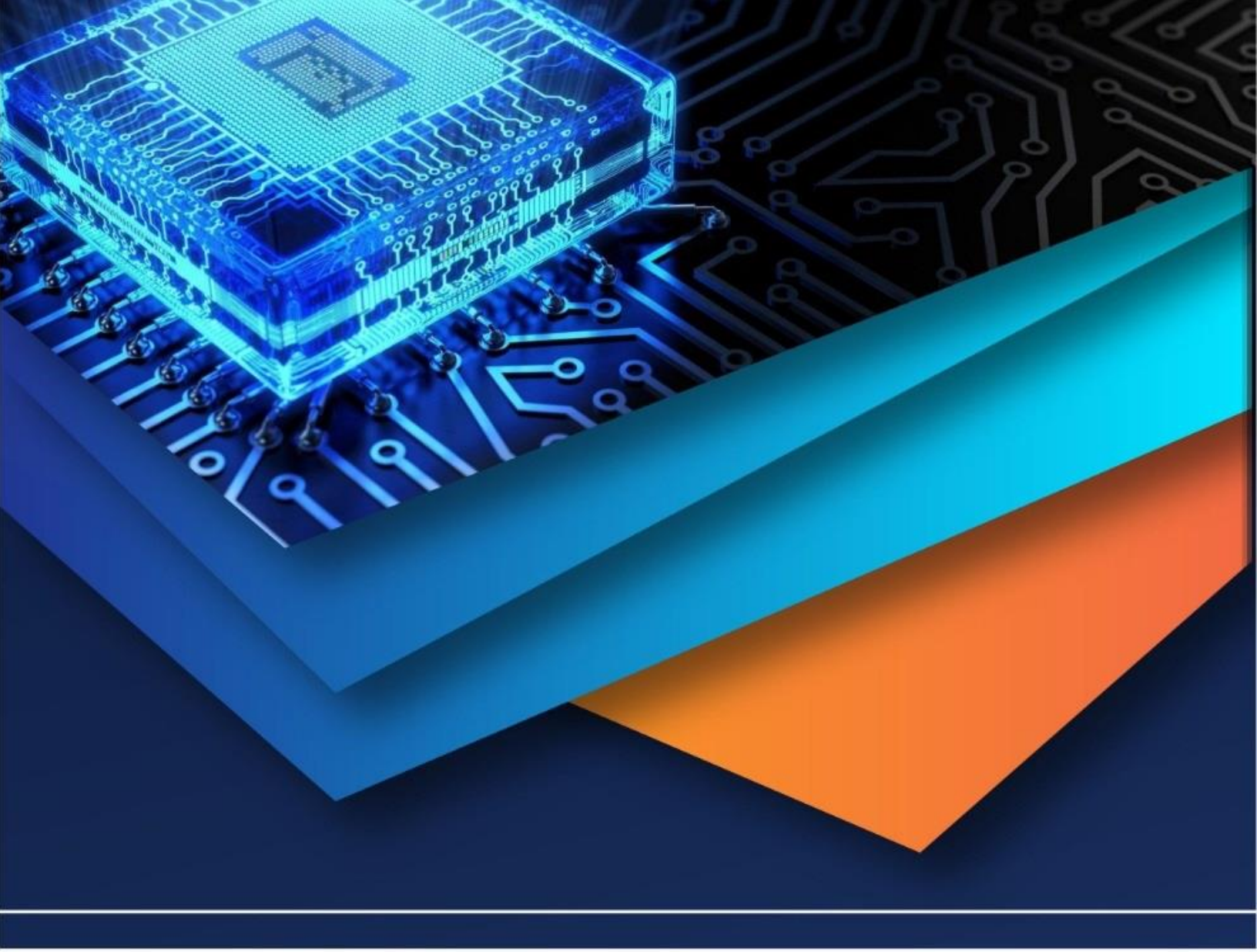
VI. SIMULATION RESULTS

In this section, we provide simulation results to evaluate the performance of the proposed schemes for perfect and
imperfect CSI for both IRA and ERA. We assume that all the nodes in the network are placed in the circle with the diameter 5 Km and $hm \rightarrow n = \iota / d\varsigma$
$m \rightarrow n$ where $dm \rightarrow n$ is the distance between transmitter m and receiver n and ι is the fading coefficient and $1 \leq \varsigma \leq 4$ where ι is taken from a normalized Rayleigh distribution. Maximum power of the ST,
SR, PT, and relays are set to 20 Watt and $N0B = 1$. We als set CPT→PR
min = 2 Bit/Sec/Hz and R, the number of relay nodes, to 15 unless otherwise stated.

REFERENCES

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: an information theoretic perspective,"*Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8,pp. 1355–1387, Oct. 1975.
[3] F. Renna, N. Laurenti, and H. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*,vol. 7, no. 4, pp. 1354–1367, Aug. 2012.
[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless

physical layer security via cooperating relays," *IEEE Trans. SignalProcess.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[5] A. Mukherjee, A. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.
[6] J. Chen, R. Zhang, L. Song, and Z. H. B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.
[7] E. Tekin and A. Yener, "The general gaussian multiple access and twoway wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 4005-4019, June 2008.
[8] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no.1,pp. 134–145, 2013.
[9] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019,Sept. 2008.
[10] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153-3167, May 2011.
[11] Y. Liang, A. Somekh-Baruch, H. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.
[12] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*,, vol. 6, no. 3, pp. 831–842, Sept. 2011.
[13] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877– 1886, June 2010.
[14] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.
[15] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.
[16] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, June 2012.
[17] K. Lee, O. Simone, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. 2011 IEEE Int. Conf. Commun.*
[18] J. Papandriopoulos and J. Evans,"Low-complexity distributedalgorithms for spectrum balancing in multi-user DSL networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 46, no. 5, pp. 3270–3275, June 2006.
[19] L. V. S. Boyd, S.-J. Kim, and A. Hassibi, "A tutorial on geometric programming," *Optimization Eng.*, vol. 7, no. 5, pp. 67–127, 2007.
[20] N. Mokari, K. Navaie, and M. G. Khoshkholgh, "Downlink radi resource allocation in OFDMA spectrum sharing environment with partial channel state information," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3482–3495, Oct. 2011.
[21] I. C. Wong and B. L. Evans, "Optimal downlink OFDMA resource allocation with linear complexity to maximize ergodic capacity," *IEEETrans. Wireless Commun.*, vol. 7, no. 3, pp. 962–971, Mar. 2008.
[22] I. Wong and B. Evans, "Optimal resource allocation in the OFDMA downlink with imperfect channel knowledge," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 232–241, 2009.
[23] M. Chiang, P. Hande, T. Lan, and C. W. Tan, "Power control in wireless cellular networks," *Foundations Trends Netw.*, vol. 2, no. 4, pp. 381–533,July 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY